Cisco HyperFlex Systems Network and External Storage Management Guide for Microsoft Hyper-V

First Published: 2020-07-16

Last Modified: 2021-01-06

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

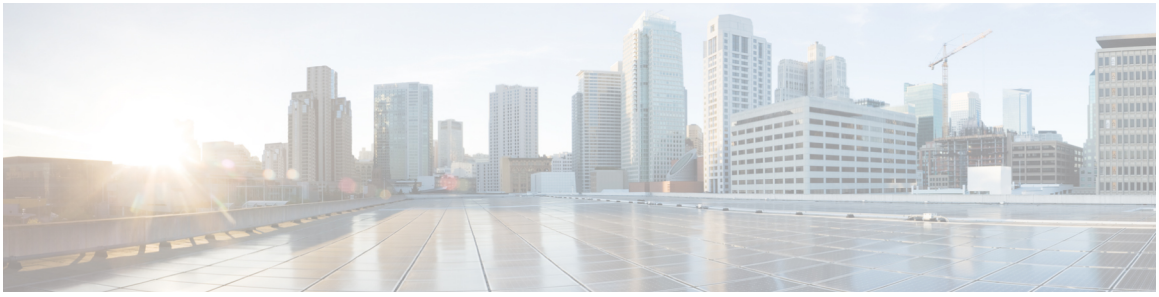
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

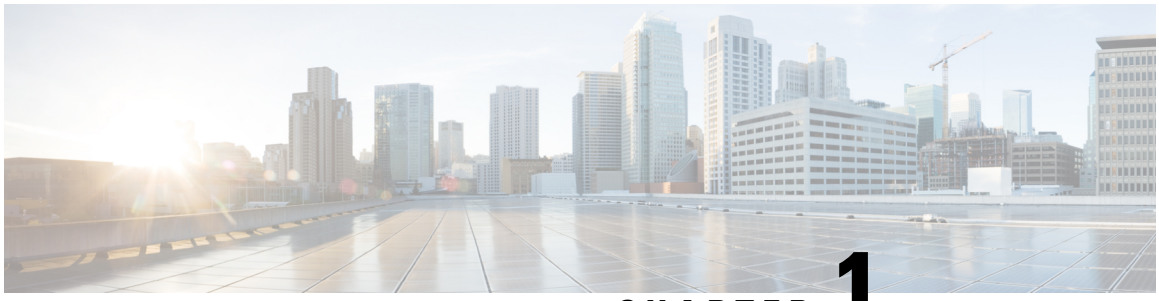
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



CONTENTS



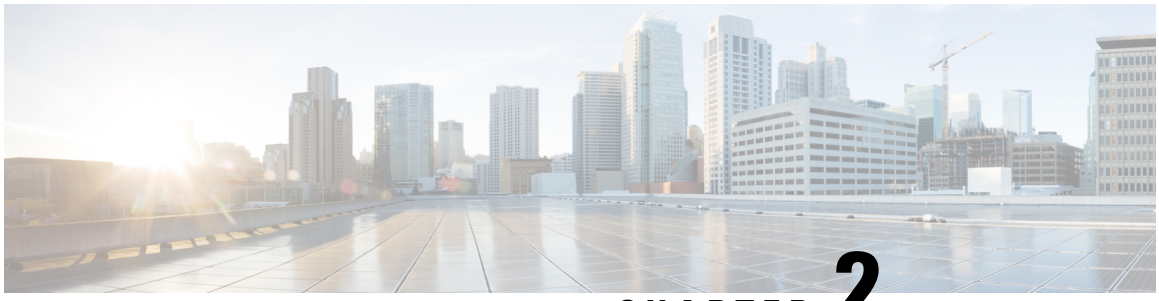
CHAPTER 1

Overview

About this Guide

This guide presents an overview of the network and external storage architecture for Cisco HyperFlex Systems. It also describes network and external management procedures that are typically performed after configuration of the initial HyperFlex cluster.

This guide is for use with all supported HX versions.



CHAPTER 2

Network Management

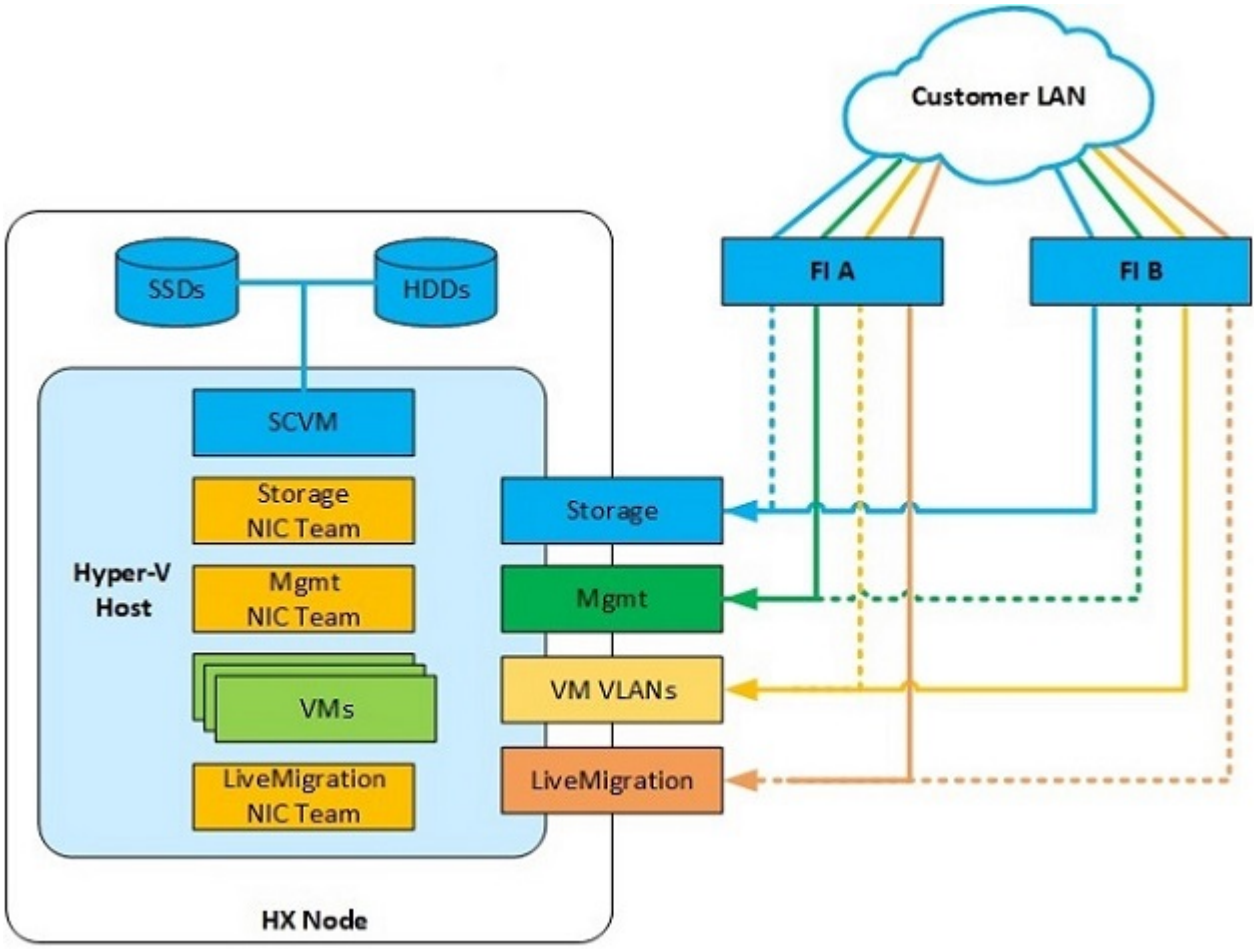
Network Design

Physical Network

Cisco UCS Uplink Connectivity

Cisco UCS network uplinks connect *northbound* from the pair of UCS Fabric Interconnects (FIs) to the LAN in the customer datacenter. All UCS uplinks operate as trunks, carrying multiple 802.1Q VLAN IDs across the uplinks. By default, the UCS software assumes that all VLAN IDs defined in the UCS configuration are eligible to trunk across all available uplinks.

Figure 1: Logical Network Design



Cisco FIs appear on the network as a collection of endpoints versus another network switch. Internally, the FIs do not participate in spanning-tree protocol (STP) domains, and the FIs cannot form a network loop, as they are not connected to each other with a layer 2 Ethernet link. The upstream root bridges make all link up/down decisions through STP.

Uplinks need to be connected and active from both FIs. For redundancy, you can use multiple uplinks on each FI, either as 802.3ad Link Aggregation Control Protocol (LACP) port-channels or using individual links. For the best level of performance and redundancy, make uplinks as LACP port-channels to multiple upstream Cisco switches using the virtual port channel (vPC) feature. Using vPC uplinks allows all uplinks to be active passing data, plus protects against any individual link failure and the failure of an upstream switch. Other uplink configurations can be redundant, but spanning-tree protocol loop avoidance may disable links if vPC is unavailable.

All uplink connectivity methods must allow for traffic to pass from one FI to the other, or from fabric A to fabric B. Scenarios can occur where cable, port, or link failures require traffic that normally does not leave the UCS domain to now be forced over the UCS uplinks. In addition, you can briefly see this traffic flow pattern maintenance procedures, such as during firmware updates on the FI, which requires them to be rebooted.

VLANs and Subnets

For a Cisco HyperFlex system configuration, you must carry multiple VLANs to the UCS domain from the upstream LAN. You define these VLANs in the UCS configuration.

Table 1: HyperFlex Installer-Created VLANs

VLAN Name	VLAN ID	Purpose
hx-inband-mgmt	Customer supplied	Hyper-V host management interfaces HX Storage Controller VM management interfaces HX Storage Cluster roaming management interface
hx-storage-data	Customer supplied	Hyper-V host storage vmkernel interfaces HX Storage Controller storage network interfaces HX Storage Cluster roaming storage interface
hx-vm-data	Customer supplied	Guest VM network interfaces
hv-livemigration	Customer supplied	Hyper-V host Live Migration vmkernel interface

Note Datacenters often use a dedicated network or subnet for physical device management. In this scenario, the mgmt0 interfaces of the two FIs must connect to that dedicated network or subnet. HyperFlex installations consider this a valid configuration with the following caveat: you must deploy the HyperFlex installer in a location where it has IP connectivity to the following subnets:

- Subnet of the mgmt0 interfaces of the FIs
- Subnets used by the hx-inband-mgmt VLANs previously listed

Jumbo Frames

Configure all Cisco HyperFlex storage traffic that traverses the hx-storage-data VLAN and subnet to use jumbo frames; that means you configure all communication to send IP packets with a Maximum Transmission Unit (MTU) size of 9000 bytes. When you use a larger MTU value, each IP packet sent carries a larger payload, so it transmits more data per packet, and consequently sends and receives data faster. This requirement also means that you must configure the Cisco UCS uplinks to pass jumbo frames. Failure to configure the Cisco UCS uplink switches to allow jumbo frames can lead to service interruptions during some failure scenarios, particularly when cable or port failures cause storage traffic to traverse the northbound Cisco UCS uplink switches.

Logical Network

The Cisco HyperFlex system has communication pathways that fall into the following defined zones:

Table 2: Defined Communication Pathway Zones

Zone	Description
Management Zone	Comprises the connections needed to manage the physical hardware, the hypervisor hosts, and the storage platform controller virtual machines (SCVM). Make these interfaces and IP addresses available to all staff who will administer the HX system, throughout the LAN/WAN. This zone must provide access to Domain Name System (DNS) and Network Time Protocol (NTP) services, and allow Secure Shell (SSH) communication.
VM Zone	Comprises the connections needed to service network IO to the guest VMs that run inside the HyperFlex hyperconverged system. This zone typically contains multiple VLANs that are trunked to the Cisco UCS Fabric Interconnects (FIs) through the network uplinks and tagged with 802.1Q VLAN IDs. Make these interfaces and IP addresses available to all staff and other computer endpoints that need to communicate with the guest VMs in the HX system, throughout the LAN/WAN.
Storage Zone	Comprises the connections used by the Cisco HX Data Platform software, Hyper-V hosts, and the storage controller VMs to service the HX Distributed Data Filesystem. These interfaces and IP addresses must be able to communicate with each other at all times for proper operation. During normal operation, this traffic all occurs within the UCS domain; however, there are hardware failure scenarios where this traffic needs to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the UCS domain, reaching FI A from FI B, and vice-versa. This zone contains primarily jumbo frame traffic, so jumbo frames must be enabled on the UCS uplinks.
Live Migration Zone	Comprises the connections used by the Hyper-V hosts to enable Live Migration of the guest VMs from host to host. During normal operation, this traffic all occurs within the Cisco UCS domain; however, there are hardware failure scenarios where this traffic needs to traverse the network northbound of the Cisco UCS domain. For that reason, the VLAN used for HX storage traffic must be able to traverse the network uplinks from the Cisco UCS domain, reaching FI A from FI B, and vice-versa.

Virtual Network

The Cisco HyperFlex system has a pre-defined virtual network design at the hypervisor level. The HyperFlex installer creates four different virtual switches (vSwitches). Each switch uses two uplinks, which are each serviced by a vNIC defined in the Cisco UCS service profile.

Figure 2: Hyper-V Network Design

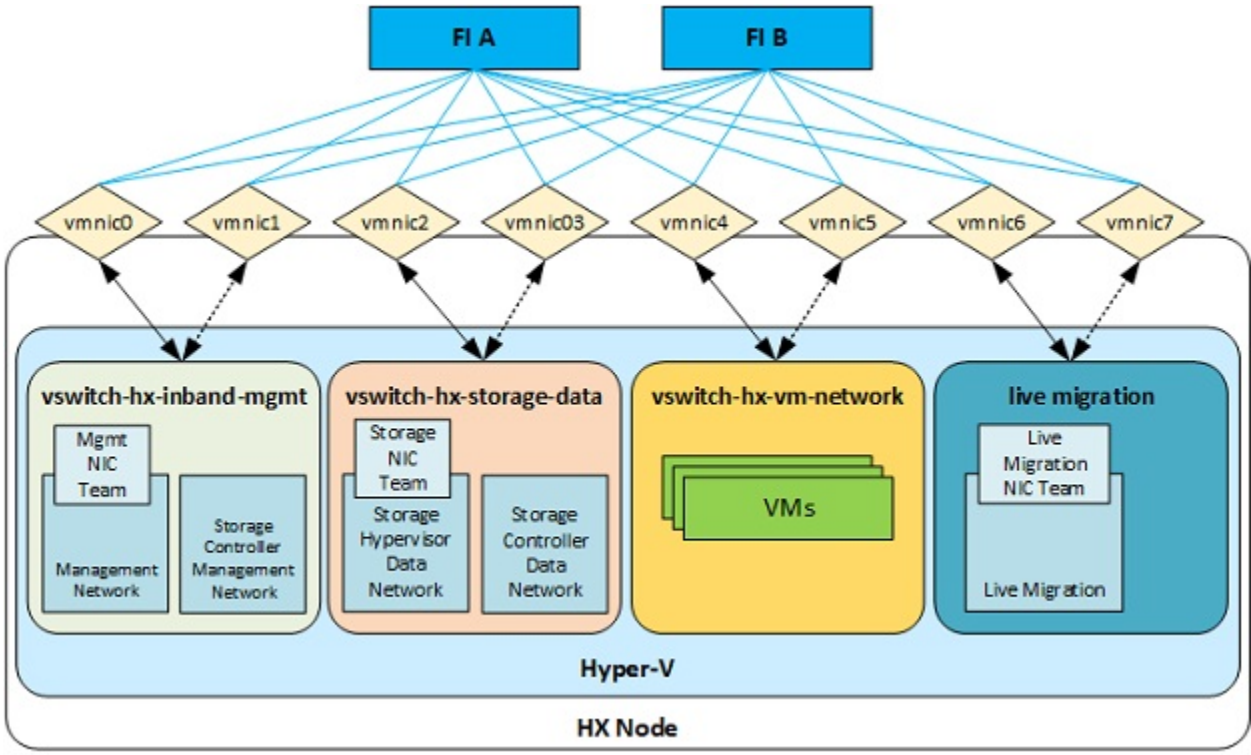


Table 3: Installer-Created vSwitches

vSwitches	Description
vswitch-hx-inband-mgmt	Default vSwitch0. Renamed by the Hyper-V kickstart file as part of the automated installation. The installer configures the default vmkernel port, vmk0, in the standard Management Network port group. The switch has two uplinks, active on fabric A and standby on fabric B, without jumbo frames. The installer also creates a second port group for the Storage Platform Controller VMs to connect to with their individual management interfaces. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V.
vswitch-hx-storage-data	Created as part of the automated installation. The installer configures a vmkernel port in the Storage Hypervisor Data Network port group. The system uses the interface for connectivity to the HX Datastores through NFS. The switch has two uplinks, active on fabric B and standby on fabric A, with jumbo frames required. The installer also creates a second port for the Storage Platform Controller VMs to connect to with their individual storage interfaces. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V.
vswitch-hx-vm-network	Created as part of the automated installation. The switch has two uplinks, active on both fabrics A and B, and without jumbo frames. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V.

vSwitches	Description
vswitch-hx-livemigration	Created as part of the automated installation. The switch has two uplinks, active on fabric A and standby on fabric B, with jumbo frames required. The VLAN is not a Native VLAN as assigned to the vNIC template, and therefore assigned in Hyper-V.

Network Configuration after Cluster Setup

Creating a QoS Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic.

You must include a QoS policy in a vNIC policy or vHBA policy, and then include that policy in a service profile to configure the vNIC or vHBA.

You can configure the system classes shown in the following table:

Table 4: System Classes

System Class	Description
Platinum Gold Silver Bronze	Configurable set of system classes that you can include in the QoS policy for a service profile. Each system class manages one lane of traffic. All properties of these system classes are available for you to assign custom settings and policies.
Best Effort	Sets the quality of service for the lane reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy that allows it to drop data packets if required. You cannot disable this system class.
Fibre Channel	Sets the quality of service for the lane reserved for Fibre Channel over Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy that ensures it never drops data packets. You cannot disable this system class. **Note** FCoE traffic has a reserved QoS system class that should not be used by any other type of traffic. If any other type of traffic has a CoS value that is used by FCoE, the value is remarked to 0.

To create a QoS Policy in UCS Manager, perform the following steps:

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 In the **Navigation** pane, click **LAN**.

Step 3 In the **LAN** tab, expand **LAN** > **Policies**.

Step 4 Expand the **root** node > **Sub-org > hx-cluster**

Step 5 Right-click **QoS Policy** and select **Create QoS Policy**.

Step 6 In the **Create QoS Policy** dialog, complete the fields for your systems class as shown in the following table:

QoS Policy Name	QoS Class	Burst Size	Rate	Host Control
Platinum	Platinum	10240	Line-rate	none
Gold	Gold	10240	Line-rate	none
Silver	Silver	10240	Line-rate	none
Bronze	Bronze	10240	Line-rate	none
Best Effort	Best Effort	10240	Line-rate	none

Step 7 Click **OK**.

What to do next

Include the QoS policy in a vNIC or vHBA template.

Creating MAC Address Pools

You can change the default MAC address blocks to avoid duplicate MAC addresses that may already exist. Each block contains 100 MAC addresses by default to allow for up to 100 HX servers for deployment per UCS system. We recommend that you use one MAC pool per vNIC for easier troubleshooting.

Note The 8th digit is set to either A or B. The *A* is set on vNICs pinned to Fabric Interconnect (FI) A. The *B* is set on vNICs pinned to FI B.

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 In Cisco UCS Manager, navigate to **LAN tab** > **Pools** > **root** > **Sub-org** > **hx-cluster** > **MAC Pools**.

Step 3 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 4 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the required fields as shown in the following table:

MAC Pool Name	**Description**	**Assignment Order**	**MAC Address block**
hv-mgmt-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:01:01-64
hv-mgmt-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:02:01-64
storage-data-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:03:01-64

storage-data-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:04:01-64
vm-network-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:05:01-64
vm-network-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:06:01-64
hv-livemigration-a	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:07:01-64
hv-livemigration-b	MAC pool for HyperFlex System	Sequential	00:25:B5:XX:08:01-64

Step 5 Click **Next**.

Step 6 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.

Step 7 In the **Create a Block of MAC Addresses** dialog box, complete the following fields:

Name	Description
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **OK**.

Step 9 Click **Finish**.

After the MAC address change, the software reconfigures Hyper-V to how it was configured earlier. But, if management IP was DHCP assigned, then the IP changes.

Impact of Manufacturing process on MAC address change

- The MAC address will change between the manufacturing process and the customer site, especially if the customer orders HyperFlex serves without UCS Fabric Interconnects.
- A MAC address is configured during Service Profile association. It is un-configured during Service Profile disassociation.
- At the end of manufacturing process, the service profiles are disassociated, hence the MAC addresses are un-configured.
- When a HyperFlex server is deployed, configure the MAC address pools as described earlier.

Creating VLANs for HX Servers

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 Navigate to **LAN tab** > **LAN** > **LAN Cloud** > **VLANS**.

Step 3 Right-click and select Create VLANs as shown in the table below:

VLAN Name	Description	Multicast Policy Name	VLAN ID (by default)
hx-inband-mgmt	Used for: • Hyper-V management • SSH to storage controller VM • HX Cluster management IP - using multicast traffic. • Hyper-V Manager connectivity to the HyperFlex VM for the HX Data Platform plug-in	HyperFlex	3091
hx-storage-data	Used for: • Hyper-V NFS client (IOvisor) • HyperFlex replication/cluster • Cluster data VIP	HyperFlex	3092
hx-livemigration	Used for: • VM and storage livemigration, FT, iSCSI	HyperFlex	3093
insert existing vlan name	Used for: • VM data traffic	HyperFlex	Any*

Note
- Configuration option is Common/Global. It applies to both fabrics and uses the same configuration parameters in both cases.
- *There is no specific recommendation for VM data VLANs. You can create your own VLANs for the VM data traffic. By default, the HXDP installer will not create VLANs for the VM data traffic.

Creating vNIC Templates for HX Servers

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- QoS policy
- LAN pin group

- Statistics threshold policy

In this procedure you create a total of eight vNIC templates: one each for the traffic management, storage management, Network Management, LiveMigration for FI(A) and same set for FI(B)

Step 1 In Cisco UCS Manager, navigate to **LAN tab** > **Policies** > **root** > **Sub-Organization** > **Hyperflex** > **vNIC Templates**.

Step 2 Right-click the **vNIC Templates** node and select **Create vNIC Template**.

Step 3 In the **Create Network Policy** dialog box, complete the required fields as follows:

vNIC Template Name	Fabric ID	VLAN	Native VLAN	MAC address Pool	MTU	QoS Policy	Network Control Policy	Description
hv-mgmt-a	A	hx-inband-mgmt	Yes	hv-mgmt-a	1500	Silver	Network Control Policy: **hyperflex-infra**	Used for: • ESX management • SSH to storage controller VM • Cluster management IP • Hyper-V manager connectivity to the HX Controller VM for the HXDP plug-in • **hv-mgmt-a** and **hv-mgmt-b** are used as uplinks for virtual switch **vswitch-hx-inband-mgmt** in Hyper-V manager
hv-mgmt-b	B	hx-inband-mgmt	Yes	hv-mgmt-b				

vNIC Template Name	Fabric ID	VLAN	Native VLAN	MAC address Pool	MTU	QoS Policy	Network Control Policy	Description
storage-data-a	A	storage-data	Yes	storage-data-a	9000	Platinum	Network Control Policy: **hyperflex-infra**	Used for: • Hyper-V NFS client (IOSvisor) • HXDP replication/cluster • Cluster data VIP • **storage-data-a** and **storage-data-b** are used as uplinks for virtual switch **vswitch-hx-storage-data** in Hyper-V manager • NFS traffic should be on a dedicated vNIC and VLAN due to security and QoS considerations
storage-data-b	B	storage-data	Yes	storage-data-b				
vm-network-a	A	(customer vlan name)	Yes	**vm-network-a**	1500	Gold	Network Control Policy: **hyperflex-vm**	Used for: • VM data traffic (VDI, database, and such) • **vm-network-a** and **vm-network-b** are used as uplinks for virtual switch **vswitch-hx-vm-network** in Hyper-V manager
vm-network-b	B	(customer VLAN name)	Yes	**vm-network-b**				
hv-livemigration-a	A	hv-motion-a	Yes	**hv-livemigration-a**	9000	Bronze	Network Control Policy: **hyperflex-infra**	Used for: • VM and storage LiveMigration, FT • **hv-livemigration-a** and **hv-livemigration-b** are used as uplinks for virtual switch **LiveMigration** in Hyper-V manager
hv-livemigration-b	B	hv-motion-b	Yes	**hv-livemigration-a**				

In the **General area**, set all the properties according to the following reference table across all the eight of the vNICs:

Failover	Disabled

Target	Adapter
Template Type	Updating
Pin Group	not set
Stats Threshold Policy	default
Dynamic vNIC Connection Policy	not set
VLANs	Configure as shown in the following table for each of the vNIC templates.

Table 5: Configured VLANs on the vNIC templates

vNIC Name	VLANs	Comments
hv-mgmt-a hv-mgmt-b	hx-inband-mgmt	The HXDP Installer configures a single VLAN on the UCSM LCP vNIC as follows: • Set the VLAN name to **hx-inband-mgmt** • Set as the native VLAN • Set the VLAN ID to 3091 by default **Note** You can change the VLAN ID in the HXDP Installer • Post HXDP install, you can open UCSM and create more VLANs to add to the **hv-mgmt-a** and **hv-mgmt-b** vNIC templates **Note** You can use these additional VLANs to access external systems, such as NetApp NFS/ISCSI filer. • Port Group name is **Storage Controller Management network** backed by VLAN **hx-inband-mgmt**
storage-data-a storage-data-b	hx-storage-data	The HXDP Installer configures a single VLAN as follows: • Set the VLAN name to **hx-storage-data** • Set as the native VLAN • Set the VLAN ID to 3092 by default **Note** You can change the VLAN id in the HXDP Installer, but it *cannot* be the same as **hx-inband-mgmt**, or the Hyper-V routing will get confused. • Port Group names are: • **Storage Controller Data Network** backed by VLAN hx-storage-data • VMK **Storage Hypervisor Data Network** backed by VLAN hx-storage-data • Subnet 10

vNIC Name	VLANs	Comments
vm-network-a vm-network-b	user created VLANs	• Manually create one or more VLANs in UCSM • Manually create port groups backed by user-created VLANs • You can create more VLANs in UCSM and assign them to the **vm-network-a** and **vm-network-b** vNIC templates for VM traffic **Note** The HXDP Installer does not configure any VLAN or Port group.
hv-livemigration-a hv-livemigration-b	hv-livemigration	The HXDP Installer configures a single VLAN as follows: • LiveMigration: VLAN **hv-livemigration-** • Set the VLAN ID • Sets as the native VLAN • VLAN ID is 3093 by default • Subnet 10

Step 4 Click **OK** when finished.

About Private VLAN

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. A private VLAN domain has only one primary VLAN. Each port in a private VLAN domain is a member of the primary VLAN, and the primary VLAN is the entire private VLAN domain.

Understanding Private VLAN Ports

The types of private VLAN ports are as follows:

- Promiscuous Primary VLAN — A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. All packets from the secondary VLANs go through this VLAN.
- Isolated Secondary VLAN — An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports.
- Community Secondary VLAN — A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.

By default, after HX deployment, a VM network uses regular VLAN.

Reset Stats Daemon

Description

A network daemon listens for statistics, like counters and timers, sent over UDP or TCP and sends aggregates to one or more pluggable backend services.

After manually re-installing Hyper-V on your HX Data Platform servers, reset the stats daemon to ensure performance statistics display correctly.

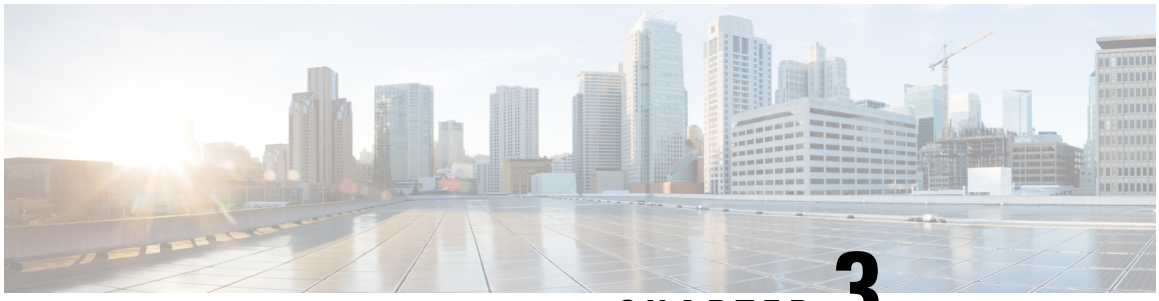
Action: restart stats daemon

Step 1 Login to the command line of the controller VM of the Hyper-V host.

Step 2 Run the restart command.

```
# /etc/init.d/statsd restart
```

Step 3 Repeat Step 1 and Step 2 on the controller VM of every Hyper-V host in the storage cluster.



CHAPTER 3

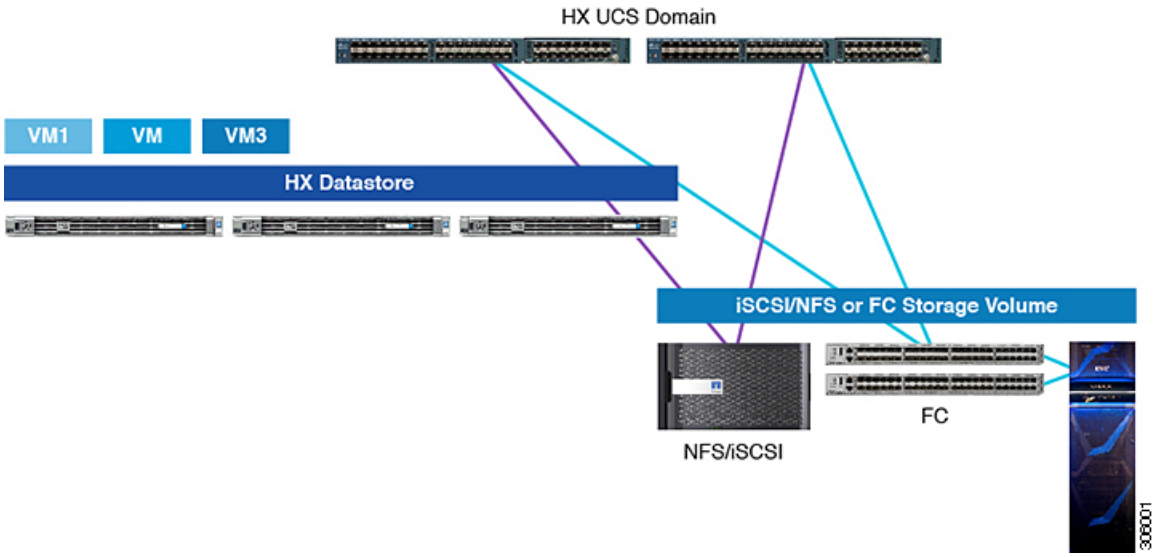
External Storage Management

Understanding External Storage Management

A Cisco HyperFlex System provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying storage access, a Cisco Unified Computing System can access storage over Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE), and iSCSI.

The following image depicts a Cisco HyperFlex System integrated with external storage.

Figure 3: Integrating External Storage with Cisco HyperFlex Systems



External Fibre Channel Storage

Fibre Channel Zoning

Fibre Channel (FC) zoning allows you to partition the FC fabric into one or more zones. Each zone defines the set of FC initiators and FC targets that can communicate with each other in a VSAN. Zoning also enables you to set up access control between hosts and storage devices or user groups.

Information About Zones

A zone consists of multiple zone members and has the following characteristics:

- Members in a zone can access each other; members in different zones cannot access each other.
- Zones can vary in size.
- Devices can belong to more than one zone.

A physical fabric can have a maximum of 8,000 zones.

Fibre Channel Zoning in Cisco UCS Manager

Cisco UCS Manager supports switch-based Fibre Channel (FC) zoning and Cisco UCS Manager-based FC zoning. You cannot configure a combination of zoning types in the same Cisco UCS domain. You can configure a Cisco UCS domain with one of the following types of zoning:

- Cisco UCS Manager-based Fibre Channel zoning — This configuration combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is performed in Cisco UCS Manager, using Cisco UCS local zoning. Any existing Fibre Channel or FCoE uplink connections need to be disabled. Cisco UCS does not currently support active Fibre Channel or FCoE uplink connections coexisting with the utilization of the Cisco UCS Local Zoning feature.
- Switch-based Fibre Channel zoning — This configuration combines direct attach storage with uplink zoning. The Fibre Channel or FCoE storage is directly connected to the fabric interconnects and zoning is performed externally to the Cisco UCS domain through an MDS or Nexus 5000 switch. This configuration does not support local zoning in the Cisco UCS domain. With switch-based zoning, a Cisco UCS domain inherits the zoning configuration from the upstream switch.

Note Zoning is configured on a per-VSAN basis. You cannot enable zoning at the fabric level.

Recommendations

- If you want Cisco UCS Manager to handle Fibre Channel zoning, the fabric interconnects must be in Fibre Channel Switch mode. You cannot configure Fibre Channel zoning in End-Host mode.
- If a Cisco UCS domain is configured for high availability with two fabric interconnects, we recommend that both fabric interconnects are configured with the same set of VSANs.

Configuring Fibre Channel Zoning

Step 1 If you have not already done so, disconnect the fabric interconnects in the Cisco UCS domain from any external Fibre Channel switches, such as an MDS.

Step 2 If the Cisco UCS domain still includes zones that were managed by the external Fibre Channel switch, run the `clear-unmanaged-fc-zone-all` command on every affected VSAN to remove those zones.

This functionality is not currently available in the Cisco UCS Manager GUI. You must perform this step in the Cisco UCS Manager CLI.

Step 3 Configure the Fibre Channel switching mode for both fabric interconnects in Fibre Channel Switch mode.

You cannot configure Fibre Channel zoning in End-Host mode. See http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/3-1/b_UCSM_GUI_Storage_Management_Guide_3_1/b_UCSM_GUI_Storage_Management_Guide_3_1_chapter_01110.html#task_B6E0C2A15FE84D498503ADC19CDB160B

Step 4 Configure the Fibre Channel and FCoE storage ports that you require to carry traffic for the Fibre Channel zones.

See Configuring an Ethernet Port as an FCoE Storage Port and Configuring a Fibre Channel Storage Port. Refer the following link:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/3-1/b_UCSM_GUI_Storage_Management_Guide_3_1/b_UCSM_GUI_Storage_Management_Guide_3_1_chapter_01100.html#task_A33D13CA58924EB1AD35EBA473B92625

Direct Attached Storage

A typical Direct Attached Storage (DAS) system is made of a data storage device connected directly to a computer through a host bus adapter (HBA). Between those two points there is no network device (like a switch or router). The main protocols used for DAS connections are ATA, SATA, eSATA, SCSI, SAS, USB, USB 3.0, IEEE 1394 and Fibre Channel.

Cisco UCS Manager allows you to have DAS without the need for a SAN switch to push the zoning configuration. The DAS configuration described assumes that the physical cables are already connected between the storage array ports and the Fabric Interconnects.

Note VSAN is created in the SAN Cloud tab, even when the storage is directly attached.

Fiber Channel Switching Mode

The Fiber Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fiber Channel switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the connected fiber channel networks, representing all servers (hosts) connected to it through virtual host bus adapters (vHBAs). This behavior is achieved by pinning (either dynamically pinned or hard pinned) vHBAs to Fiber Channel uplink ports, which makes the Fiber Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fiber Channel Switching mode.

Note When you enable end-host mode, if a vHBA is hard pinned to an uplink Fiber Channel port and this uplink port goes down, the system cannot re-pin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is the traditional Fiber Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fiber Channel switch mode is useful in Pod models where there is no SAN (for example, a single Cisco UCS domain that is connected directly to storage), or where a SAN exists (with an upstream MDS). Switch mode is not the default Fiber Channel switching mode.

Note In Fiber Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fiber Channel Switching Mode

Important When you change the Fiber Channel switching mode, Cisco UCS Manager logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Manager restarts both fabric interconnects simultaneously. The second fabric interconnect can take several minutes to complete the change in Fiber Channel switching mode and become system ready.

When the Fiber Channel switching mode is changed, both Cisco UCS fabric interconnects will reload simultaneously. Reloading of fabric interconnects will cause a system-wide downtime for approximately 10-15 minutes.

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name**.

Step 3 In the Work pane, click the **General** tab.

Step 4 In the **Actions** area of the **General** tab, click one of the following links:

- **Set FC Switching Mode**
- **Set FC End-Host Mode**

The link for the current mode is dimmed.

Step 5 In the dialog box, click **Yes**.

Cisco UCS Manager restarts the fabric interconnect, logs you out, and disconnects Cisco UCS Manager GUI.

Connect FC Storage Connection to FI and Configure as a FC Storage Port

In the UCS Manager, perform the following steps:

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name**.

Step 3 Click the ports under the FC Port node.

Step 4 Right-click the selected port(s) and choose **Configure as FC Storage Port**.

Step 5 In the dialog box, click **Yes**.

Step 6 Click **OK**.

Creating VSAN for Fibre Channel

FCoE VLANs in the SAN cloud and VLANs in the LAN cloud must have different IDs. Using the same ID results in a critical fault and traffic disruption for all vNICs and uplink ports that use that FCoE VLAN. Ethernet traffic is dropped on any VLAN with an ID that overlaps with an FCoE VLAN ID.

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Click the **SAN Cloud > VSAN** node.

Step 3 Right-click the **VSAN** node, and select **Create Storage VSAN**.

Step 4 In the **Create VSAN** dialog box, complete the following fields:

Name	Description
Name field	The name assigned to the network. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
FC Zoning* field	Select **Enable** radio button for FC Switch mode. The HX Installer may disable it during the configuration process, verify that it is enabled at the end of the configuration. **Note** Make sure that the FI is not connected to an upstream switch.

Name	Description
Configuration	Select a configuration for your environment. • Click the **Common/Global** radio button so that VSAN maps to the same VSAN ID in all available fabrics. • Click **Both Fabrics Configured Differently** radio button to create two VSANS, with different IDs for Fabric A and Fabric B.
VSAN ID field	The unique identifier assigned to the network. For FC end-host mode, the range between 3840 to 4079 is also a reserved VSAN ID range.
FCoE VLAN field	The unique identifier assigned to the VLAN used for Fibre Channel connections. VLAN 4048 is user configurable. However, Cisco UCS Manager uses VLAN 4048 for the following default values. If you want to assign 4048 to a VLAN, you must reconfigure these values.

What to do next

If you need to create a new HX cluster, go to: Configuring External Storage on a New Cluster with HX Installer, on page 22. If the HX cluster is already created, go to: Configuring External Storage on an Existing Cluster, on page 23

Configuring External Storage on a New Cluster with HX Installer

If the HX cluster is not yet created, perform the following steps to add vHBA and VSAN with HX Installer.

Step 1 In the HX Data Platform installer on the UCSM Configuration page, check the **Enable FC Storage** option.

Step 2 In the FC Storage box, complete the following fields:

Field Name	Description	Example Value
FC Storage	Check box that indicates if FC Storage should be enabled.	Check the box to enable FC Storage
wWxN Pool	A WWM pool that contains both WW node names and WW Port names. For each fabric interconnect, a WWxN pool is created for WWPN and WWNN.	20:00:25:B5:C2
VSAN A Name	the name of the VSAN for the primary fabric interconnect (FI-A). By default, this is set to hx-ext-storage-fc-a.	hx-ext-storage-fc-a
VSAN A ID	The unique identifier assigned to the network for the primary fabric interconnect (FI-A)	70

Field Name	Description	Example Value
VSAN B Name	The name of the VSAN for subordinate fabric interconnect (FI-B)	hx-ext-storage-fc-b
VSAN B ID	The unique identifier assigned to network for subordinate fabric interconnect (FI-B)	70

Step 3 Allow the HX Installer complete the cluster creation.

What to do next

configure Fibre Channel Zoning, on page 18.

Configuring External Storage on an Existing Cluster

If the HX Cluster is already Created, you may use the following tasks to add vNics and VSAN manually.

Creating WWNN Pools

A World Wide Node Name (WWNN) pool is a World Wide Name (WWN) pool that contains only World Wide Node Names. If you include a pool of WWNNs in a service profile, the software assigns the associated server a WWNN from that pool.

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, it is recommended to use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **Pools** > **root** > **Sub-Organizations** > **hx-cluster**.

Step 3 Expand the **hx-cluster** sub-organization to create the pool.

Step 4 Right-click WWNN Pools and select **Create WWNN Pool**.

Step 5 In the **Define Name and Description** dialog box of the **Create WWNN Pool** wizard, enter **`HyperFlex`**.

Step 6 Click **Next**.

Step 7 In the **Add WWN Blocks** page of the **Create WWNN Pool** wizard, click **Add**.

Step 8 In the **Create WWN Block** dialog box, complete the following fields:

Form field: The first WWN in the block.

Size field: The number of WWNs in the block.

For WWN pools, the pool size must be a multiple of ports-per-node + 1. For example, if there are seven ports per node, the pool size must be a multiple of eight. If there are 63 ports per node, the pool size must be a multiple of 64.

Step 9 Click **OK**.

Step 10 Click **Finish**.

What to do next

Create WWPN Pool.

Creating a WWPN Pool

To create a WWWPN Pool, perform the following steps.

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **Pools** > **root** > **Sub-Organizations** > **hx-cluster**.

Step 3 Right-click WWPN Pools and select **Create WWPN Pool**.

Step 4 In the **Define Name and Description** dialog box of the **Create WWPN Pool** wizard, enter **`hx-a`**.

Step 5 Click **Next**.

Step 6 In the **Add WWN Blocks** page of the **Create WWNN Pool** wizard, click **Add**.

Step 7 In the **Create WWN Block** dialog box, complete the following fields:

Form field: The first WWN in the block.

Size field: The number of WWNs in the block.

For WWN pools, the pool size must be a multiple of ports-per-node + 1. For example, if there are seven ports per node, the pool size must be a multiple of eight. If there are 63 ports per node, the pool size must be a multiple of 64.

Step 8 Click **OK**.

Step 9 Click **Finish**.

What to do next

Create WWPN Pool **hx-b**. Follow the steps above.

Creating a vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template. Include this policy in a service profile for it to take effect.

Before you begin

Before creating the vHBA template policy, make sure that one or more of the following resources exist in the system:

- Named VSAN
- WWNN pool or WWPN pool
- SAN pin group
- Statistics threshold policy

Step 1 In the **Navigation** pane, click **SAN**.

Step 2 Expand **SAN** > **Policies** > **root** > **Sub-Organizations** > **hx-cluster**.

Step 3 Right-click the **vHBA Templates** node and choose **Create vHBA Template**.

Step 4 In the **Create vHBA Template** dialog box, complete the following fields:

Name	Description
Name field	Enter **vhba-a**. The name of the virtual HBA template. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than hyphen (-), underscore(_), period(.), and colon (:). You cannot change this name after the object is saved.
Description field	Enter up to 256 characters. A user-defined description of the template.
Fabric ID field	Select **A**.
Select VSAN drop-down list	Select the VSAN created earlier for Fabric A, to associate with this vHBA.
Template Type field	Select **Updating Template**. vHBAs created from this template are updated if the template changes.
Max Data Field Size field	Default: 2048 This the maximum size of the Fibre Channel frame payload bytes that the vHBA supports.
WWPN Pool drop-down list	Assign **hx-a**.
QoS Policy drop-down list	*<Not set>*
Pin Group drop-down list	*<Not set>*
Stats Threshold Policy drop-down list	*<Not set>*

Step 5 Click **Ok**.

What to do next

Create vHBA template for fabric interconnect B.

SAN Connectivity Policy

Connectivity policies determine the connections and the network communication resources between the server and the SAN in the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates. Also, connectivity policies can be used to configure multiple servers.

Including SAN Connectivity Policy to the HX Node Service Profile Template

Step 1 In the **Navigation** pane, click **Server**.

Step 2 Expand **Servers** > **Service Profile Template** > **root** > **Sub-Organizations** > **hx-cluster**.

Step 3 Select **`Service Template hx-nodes`**, select **`vHBA`**.

Step 4 In the work pane, on **Storage** tab, select **`HyperFlex`** from the drop-down list under the **SAN Connectivity Policy** section.

Step 5 Click **Save**.

This causes the Service Profiles associated with this SPT to require user acknowledgement and the HX node reboots.

Adding vNICs or vHBAs to a Hyper-V Deployed HyperFlex Cluster

To add additional storage such as FlexPod, after installing your HyperFlex cluster, use the following procedure. Do not reboot multiple nodes at once after making these hardware changes. Validate the health state of each node before rebooting or performing the procedure on subsequent nodes.

To add Virtual Network Interface Controllers (vNIC) or Virtual Host Bus Adapters (vHBA) to a deployed HyperFlex cluster, complete the following steps:

Before you begin

For vHBAs, you will need to download the driver from the Cisco Download Software site and install it.

Step 1 Add vHBAs to the service profile templates for HyperFlex. See Creating a vHBA Template , on page 24 for more details.

Important After you add vHBAs to the service profile template, the HX servers indicate that a reboot is required. Do *not* reboot the HX servers now.

Note Download and install the vHBA drivers, from Cisco Software Download.

Step 2 Use the HX Connect UI to enter the maintenance mode. See the *Cisco HyperFlex Data Platform Administration Guide for Hyper-V* for more information.

Step 3 After the system enters maintenance mode, reboot the associated node in Cisco UCS Manager to complete the addition of new hardware.

Step 4 Reboot the host.

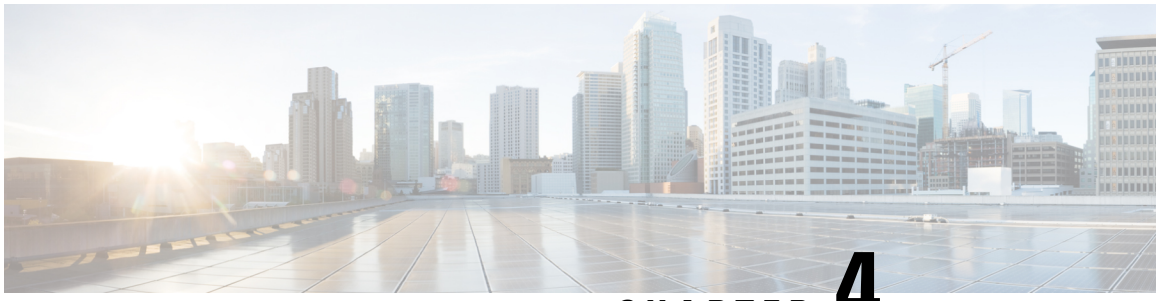
Step 5 Use the HX Connect UI to exit the maintenance mode. See the *Cisco HyperFlex Data Platform Administration Guide for Hyper-V* for more information.

Step 6 Check the health status of the HyperFlex cluster and confirm that the cluster is healthy before proceeding to the next node.

```
# hxcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

Step 7 Repeat the process for each node in the cluster as necessary.



CHAPTER 4

iSCSI

iSCSI SAN Concepts

iSCSI SANs use Ethernet connections between computer systems, or host servers, and high performance storage subsystems. SAN components include iSCSI Host Bus Adapters (HBAs) or Network Interface Cards (NICs) in the host servers, switches, and routers that transport the storage traffic, cables, storage processors, and storage disk systems.

iSCSI SAN uses a client-server architecture. The client, called iSCSI initiator, operates on the host. It initiates iSCSI sessions by issuing iSCSI commands and transmits them, encapsulated using the iSCSI protocol, to a server. The server is known as the iSCSI target. The iSCSI target represents a physical storage system on the network. It can also be provided by a virtual iSCSI SAN, for example, an iSCSI target emulator running in a virtual machine. The iSCSI target responds to the initiator's commands by transmitting the required iSCSI data.

Connecting iSCSI to Cisco HX Domain

Connect FC Storage Connection to FI and Configure as a FC Storage Port

In the UCS Manager, perform the following steps:

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name**.

Step 3 Expand the node for the ports that you want to configure.

Step 4 Under the **Ethernet Ports** node, select a port.

Step 5 Select **Configure as Appliance Port** from the drop-down list.

a) If a confirmation dialog box appears, click **Yes**.

Step 6 In the **Configure as Appliance Port** dialog box, complete the required fields.

Step 7 In the **VLANs** section, do the following:

a) In the **Port Mode** field, you can click the **Create VLAN** link to create a new VLAN.

Access—Cisco UCS Manager GUI displays the Select VLAN drop-down list that allows you to choose a VLAN to associate with this port or port channel.

Note If traffic for the appliance port needs to traverse the uplink ports, you must also define each VLAN used by this port in the LAN cloud. For example, you need the traffic to traverse the uplink ports if the storage is also used by other servers, or if you want to ensure that traffic fails over to the secondary fabric interconnect if the storage controller for the primary fabric interconnect fails.

b) Choose a VLAN from the **Select VLAN** drop-down list.

Step 8 Click **OK**.

Creating VLAN for Adding iSCSI Storage to HX FI Domain

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 Navigate to **LAN tab** > **LAN** > **LAN Cloud** > **VLANS**.

Step 3 Right-click and select **Create VLANs** as shown in the following table:

VLAN Name	Description	Multicast Policy Name	VLAN ID (by default)
hx-extstorage-iscsi	Used for adding external storage connectivity	HyperFlex	Sample Value: 4201

Note
- Configuration option is Common/Global. It applies to both fabrics and uses the same configuration parameters in both cases.
- Sharing type is set to None.

Step 4 Click **Ok**.

Configuring External Storage on a New Cluster with HX Installer Missing

If the HX cluster is not yet created, perform the following steps to add vNIC and VLAN for iSCSI traffic.

SUMMARY STEPS

1. In the HX Data Platform installer on the UCSM Configuration page, check the **Enable HX** option.
2. In the **iSCSI Storage** box, check the **Enable iSCSI Storage** checkbox.

DETAILED STEPS

Step 1 In the HX Data Platform installer on the UCSM Configuration page, check the **Enable HX** option.

The **iSCSI Storage** box appears.

Step 2 In the **iSCSI Storage** box, check the **Enable iSCSI Storage** checkbox.

Configuring External Storage on an Existing Cluster

If the HX Cluster is already Created, you may use the following tasks to add vNics and VSAN manually.

Creating MAC Address Pools for External Storage

Change the default MAC address blocks to avoid duplicate MAC addresses that already exist. Each block contains **100 MAC addresses** by default to allow for up to 100 HX servers for deployment per UCS system. We recommend that you use one MAC pool per vNIC for easier troubleshooting.

Note The 8th digit is set to A or B. The *A* is set on vNICs pinned to Fabric Interconnect (FI) A. The *B* is set on vNICs pinned to FI B.

Step 1 Open a web browser and enter the IP address for Cisco UCS Manager. Enter the login credentials.

Step 2 In Cisco UCS Manager, navigate to **LAN tab** > **Pools** > **root** > **Sub-org** > **hx-cluster** > **MAC Pools**.

Step 3 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 4 In the **Define Name and Description** page of the **Create MAC Pool** wizard, complete the required fields as shown in the following table:

MAC Pool Name	**Description**	**Assignment Order**	**MAC Address block**
hx-extstorage-a	MAC pool for adding external storage to HyperFlex System	Sequential	00:25:B5:XX:01:01-63

Note Make sure to check the last block of MAC addresses and use next order of block to create the new MAC pools for both fabrics.

Step 5 Click **Next**.

Step 6 In the **Add MAC Addresses** page of the **Create MAC Pool** wizard, click **Add**.

Step 7 In the **Create a Block of MAC Addresses** dialog box, complete the following fields:

Name	**Description**
First MAC Address field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 8 Click **OK**.

Step 9 Click **Finish**.

What to do next

Repeat steps to create MAC Pool - **hx-extstorage-b** for FI b.

Creating a vNIC Template for iSCSI Storage

This template is a policy that defines how the vNIC on a server connects to the LAN. It is also called a vNIC LAN connectivity template. You must include this policy in a service profile for it to take effect.

Before you begin

This policy requires that one or more of the following resources already exist in the system:

- Named VLAN
- MAC pool
- Jumbo MTU
- QoS policy

Step 1 In Cisco UCS Manager, navigate to **LAN tab > Policies > root > Sub-Organization > Hyperflex > vNIC Templates**.

Step 2 Right-click the **vNIC Templates** node and choose **Create vNIC Template**.

Step 3 In the **Create vNIC Template** dialog box, complete the following fields:

Name	Description
Name field	Enter **extstorage_iscsi-a** This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	A user-defined description of the template. Enter up to 256 characters.
Fabric ID field	Select **A**
Redundancy drop-down list	Primary
Target	Adapter
Template Type field	Select **Updating Template**. vNICs created from this template are updated if the template changes.
VLAN field	hx-extstorage-iscsi (what you created above)
CDN Source	vNIC Name
MTU drop-down list	**9000**

Name	Description
MAC Pool	**hx-extstorage-a** (created earlier)
QoS Policy drop-down list	**Bronze**
Connection	**Dynamic**

Step 4 Click **Ok**.

What to do next

Create the vNIC template for FI B.

LAN Connectivity Policy

Connectivity policies determine the connections and the network communication resources between the server and the LAN in the network. These policies use pools to assign MAC addresses, to servers and to identify the vNICs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates. Also, connectivity policies can be used to configure multiple servers.

Creating a LAN Connectivity Policy

Step 1 In the Navigation pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN > Sub-Org > hx-cluster > LAN Connectivity Policies> HyperFlex**.

Step 3 Click **Add vNICs**.

Step 4 In the **Create vNIC** dialog box, enter a name. **Check Use vNIC Template** and **Redundancy Pair**.

Example: iscsi-A

Step 5 Enter **Peer Name**.

Example: iscsi-B

Step 6 Select **vNIC Template** name *iscsi-A* from the drop-down list. Click **Ok**.

Step 7 Repeat steps 3 - 6 to create vNIC *iscsi-B* and assign *vNIC-b* template to it.

Step 8 Click **Save Changes**. In the Save Changes box that displays, click **Yes** to accept the changes.
Includes the LAN connectivity policy to the HX node service profile template.

Including LAN Connectivity Policy to the HX Node Service Profile Template

Step 1 Navigate to **Server** tab. Expand **root > Sub-Org > hx-cluster > Service Template hx-nodes**

Step 2 In the work pane, on **Network** tab, select **`HyperFlex`** from the drop-down list under the **LAN Connectivity Policy** section.

Step 3 Click **Modify vNIC/HBA Placement**. Check the iscsi vNIC for proper order. Make sure they are last in the order. Re-arrange as necessary.

Note If you are adding both FC and iSCSI storage, then the order of vHBAs will precede the order of the vNICs.

Step 4 Click **Save**.

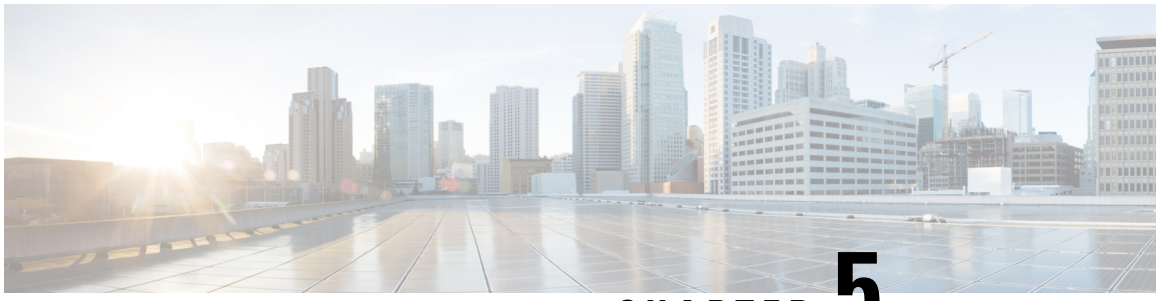
This causes the Service Profiles associated with this SPT to require user acknowledgment and the HX node re-boots.

Adding Network Adapters for Hyper-V

Step 1 Open the Windows **Device Manager**.

Step 2 Right-click on **Network Adapters**.

Step 3 Scan the system for all hardware changes.



CHAPTER 5

Connecting Cisco HX Servers to SMB and CIFS Storage

SMB and CIFS Storage Guidelines and Requirements

When using SMB or CIFS storage, use the following configuration, networking, and SMB or CIFS datastore guidelines.

SMB or CIFS Server Configuration Guidelines

- When configuring SMB or CIFS storage, follow the recommendation of your storage vendor.
- Ensure that the SMB or CIFS volume is exported using SMB or CIFS over TCP.
- Ensure that each host has root access to the volume. If the NAS server does not grant root access, you might still be able to mount the SMB or CIFS datastore on the host. However, you will not be able to create any virtual machines on the datastore.
- Make sure that the SMB or CIFS server does not provide both protocol versions for the same share.

NFS Networking Guidelines

- For network connectivity, the host requires a standard network adapter.
- If you use multiple ports for SMB or CIFS traffic, make sure that you correctly configure your virtual switches and physical switches. For information, see the vSphere Networking documentation.

Note For details on configuring SMB or CIFS storage, consult your storage vendor documentation.

Setup SMB or CIFS Storage Environment for Hyper-V

Step 1 On the Windows machine, right click on **This PC** and choose **Map Network Drive**.

Step 2 Enter the target server IP address and the path for the address.

Step 3 Click **OK**.